Claims

1. In a network, a method of maintaining at least one database to be used to categorize e-mail messages received in a network comprising:

a) receiving information about an e-mail message sent to a recipient within an e-mail network, wherein the information includes at least one of the following:

i) an actual sender of the message;

ii) a final IP address used by the sender;

iii) a final domain name used by the sender; and

iv) an IP path used by the sender;

b) storing the information; and

c) maintaining statistics based on the stored information, wherein the statistics are used to determine whether the received e-mail is unsolicited e-mail; wherein the at least one database includes one of the following:

i) a central database;

ii) at least two-centrally-maintained databases, each storing and compiling different information and statistics; and

iii) a local database.

2. The method of claim 1 wherein the actual sender is identified by a signature that includes at least two of the following fields from the message header:

a) an e-mail address used by the sender;

b) a display name used by the sender;

c) a domain name used by the sender;

d) the final IP address used by the sender;
e) the final domain name used by the sender;
f) the name of client software used by the actual sender;
g) user-agent;
h) timezone;
i) source IP address;
j) sendmail version used by a first receiver; and
k) the IP path used to route the message.

3. The method of claim 1 wherein the actual sender is identified by a signature including a range of IP addresses and at least one of the following fields from the message header:

a) an e-mail address used by the sender;
b) a display name used by the sender;
c) a domain name used by the sender;
d) the final IP address used by the sender;
e) the final domain name used by the sender;
f) the name of client software used by the actual sender;
g) user-agent;
h) timezone;
i) source IP address;
j) sendmail version used by a first receiver; and
k) the IP path used to route the message.

4. The method of claim 1 further comprising sending information about received messages to the at least one database, the information including at least two of the following:

a) information identifying the actual sender;

b) whether the actual sender is included on a recipient's whitelist;

c) whether the actual sender is included on a recipient's blacklist;

d) information identifying the final IP address;

e) whether the final IP address is included on the recipient's whitelist;

f) whether the final IP address is included on the recipient's blacklist;

g) information identifying the final domain name;

h) whether the final domain name is included on the recipient's whitelist;

i) whether the final domain name is included on the recipient's blacklist;

j) information identifying the IP path;

k) whether the IP path is included on the recipient's whitelist;

l) whether the IP path is included on the recipient's blacklist;

m) whether the message could be categorized locally; and

n) whether a recipient changed a whitelist/blacklist status of the message.

5. The method of claim 1 further comprising sending the recipient statistics about at least one of the following:

a) an actual sender;
b) a final IP address;
c) a final domain name;
d) an IP path.

6. The method of claim 1 wherein information stored about an actual sender includes at least one of the following:

a) a total number of messages sent;

b) a number of messages sent over a first predetermined time period;

c) a total number of messages sent to recipients in the network who have included the actual sender on a whitelist;

d) a number of messages sent to recipients in the network who have included the actual sender on the whitelist over a second predetermined time period;

e) a number of recipients who know the actual sender;

f) a total number of times a recipient changed an actual sender's whitelist/blacklist status;

g) a number of times a recipient changed an actual sender's whitelist/blacklist status over a third predetermined time period;

h) a total number of messages sent to recipients in the network who don't know the actual sender;

i) a number of messages sent to recipients in the network who don't know the actual sender over a fourth predetermined time period;

j) a total number of unique recipients in the network who have received at least one message from the actual sender;

k) a total number of messages sent to unique recipients in a network who have included the actual sender on a whitelist; and

l) a total number of messages sent to unique recipients in the network who have not included the actual sender on the whitelist.

7. The method of claim 1 wherein information stored about messages sent from a final IP address includes at least one of the following:

a) a total number of messages sent;

b) a number of messages sent over a first predetermined time period;

c) a total number of messages sent to recipients in the network who have included a sender on a whitelist;

d) a number of messages sent to recipients in the network who have included the sender on the whitelist over a second predetermined time period;

e) a number of recipients who have whitelisted senders having the final IP address;

f) a total number of times a recipient changed a whitelist/blacklist status of any sender using the final IP address;

g) a number of times a recipient changed the whitelist/blacklist status of any sender using the final IP address over a third predetermined time period;

h) a total number of messages sent to recipients in the network who have not included the sender on the whitelist;

i) a number of messages sent to recipients in the network who have not included the sender on the whitelist over a fourth predetermined time period;

j) a total number of unique recipients in the network who have received at least one message from at least one sender using the final IP address;

k) a total number of messages sent to unique recipients in the network who have included the sender on the whitelist; and

l) a total number of messages sent to unique recipients in the network who have not included the sender on the whitelist.

8. The method of claim 1 wherein information stored about messages sent from a final domain name includes at least one of the following:

a) a total number of messages sent;

b) a number of messages sent over a first predetermined time period;

c) a total number of messages sent to recipients in a network who have included a sender on a whitelist;

d) a number of messages sent to recipients in the network who have included the sender on the whitelist over a second predetermined time period;

e) a number of recipients who have whitelisted senders using the final domain name;

f) a total number of times a recipient changed a whitelist/blacklist status of any sender using the final domain name;

g) a number of times a recipient changed the whitelist/blacklist status of any sender using the final domain name over a third predetermined time period;

h) a total number of messages sent to recipients in the network who have not included the sender on the whitelist;

i) a number of messages sent to recipients in the network who have not included the sender on the whitelist over a fourth predetermined time period;

j) a total number of unique recipients in the network who have received at least one message from at least one sender using the final domain name;

k) a total number of messages sent to unique recipients in the network who have included the sender on the whitelist; and

l) a total number of messages sent to unique recipients in the network who have not included the sender on the whitelist.

9. The method of claim 1 wherein information stored about messages sent using an IP path includes at least one of the following:

a) a total number of messages sent;

b) a number of messages sent over a first predetermined time period;

c) a total number of messages sent to recipients in the network who have included a sender on a whitelist;

d) a number of messages sent to recipients in the network who have included the sender on the whitelist over a second predetermined time period;

e) a number of recipients who have whitelisted senders using the IP path;

f) a total number of times a recipient changed a whitelist/blacklist status of any sender using the IP path;

g) a number of times a recipient changed the whitelist/blacklist status of any sender using the IP path over a third predetermined time period;

h) a total number of messages sent to recipients in the network who have not included the sender on the whitelist;

i) a number of messages sent to recipients in the network who have not included the sender on the whitelist over a fourth predetermined time period;

j) a total number of unique recipients in the network who have received at least one message from at least one sender using the IP path;

k) a total number of messages sent to unique recipients in the network who have included the sender on the whitelist; and

l) a total number of messages sent to unique recipients in the network who have not included the sender on the whitelist.

10. The method of claim 1 wherein compiling statistics includes at least one of the following:

a) determining a ratio of a first number e-mail messages sent by an actual sender to recipients in the network who have included the sender on the whitelist in a predetermined time period divided by a second number of e-mail messages sent by an actual sender to users in the network in the predetermined time period;

b) determining a ratio of a first number of recipients in the network who have included the sender on the whitelist divided by a second number of unique recipients in the network who received e-mails from the actual sender in a predetermined time period;

c) determining a ratio of a first number of times in a predetermined time interval a message from the actual sender was moved from a whitelist to a blacklist divided by a second number of times a message from the actual sender was moved from a whitelist to a blacklist;

d) determining a ratio of a first number of times in a predetermined time interval a message from the actual sender was moved from a blacklist to a whitelist divided by a second number of times a message from the actual sender was moved from a blacklist to a whitelist;

e) determining a ratio of a first number of unique users within the network who whitelisted the actual sender within a predetermined time period compared to a second number of unique users within the network who blacklisted the actual sender within the predetermined time period;

f) determining a ratio reflecting whether the actual sender sends a majority of messages to recipients who have included the actual sender on the whitelist;

g) determining a ratio reflecting a first number of wanted messages sent by the actual sender compared to a second number of unwanted or total messages sent by the actual sender;

h) determining a difference between a first number of expected messages sent by the actual sender and a second number of unexpected ed messages sent by the actual sender;

i) determining a difference between a first number of times a user whitelisted a messages the actual sender and a second number of times a user blacklisted a message from the actual sender;

j) determining a difference reflecting whether the actual sender sends a majority of messages to known recipients;

k) converting any of the above ratios or differences to a score indicating the likelihood the message is unsolicited e-mail; and

l) applying the score to the appropriate message in the spam folder.

11. The method of claim 1 wherein compiling statistics includes at least one of the following:

a) determining a ratio of a first number e-mail messages sent by any sender using a final IP address to recipients in the network who have included the sender on the whitelist in a predetermined time period divided by a second number of e-mail messages sent by an any sender using the final IP address to users in the network in the predetermined time period;

b) determining a ratio of a first number of recipients in the network who have included the sender on the whitelist divided by a second number of unique recipients in the network who received e-mails from any sender using the final IP address in a predetermined time period;

c) determining a ratio of a first number of times in a predetermined time interval a message from any sender using the final IP address was moved from a whitelist to a blacklist divided by a second number of times a message from any sender using the final IP address was moved from a whitelist to a blacklist;

d) determining a ratio of a first number of times in a predetermined time interval a message from any sender using the final IP address was moved from a blacklist to a whitelist divided by a second number of times a message from any sender using the final IP address was moved from a blacklist to a whitelist;

e) determining a ratio of a first number of unique users within the network who whitelisted any sender using the final IP address within a predetermined time period compared to a second number of unique users within the network who blacklisted any sender using the final IP address within the predetermined time period;

f) determining a ratio reflecting whether any sender using the final IP address sends a majority of messages to recipients who have included the sender on the whitelist;

g) determining a ratio reflecting a first number of wanted messages sent by any sender using the final IP address compared to a second number of unwanted or total messages sent by any sender using the final IP address;

h) determining a difference between a first number of expected messages sent by any sender using the final IP address and a second number of unexpected messages sent by any sender using the final IP address;

i) determining a difference between a first number of times a user whitelisted a message from any sender using the final IP address and a second number of times a user blacklisted a message from any sender using the final IP address;

j) determining a difference reflecting whether any sender using the final IP address sends a majority of messages to recipients who have included the sender on the whitelist;

k) converting any of the above ratios or differences to a score indicating the likelihood the message is unsolicited e-mail; and

l) applying the score to the appropriate message in the spam folder.

12. The method of claim 1 wherein compiling statistics includes at least one of the following:

a) determining a ratio of a first number e-mail messages sent by any sender using a final domain name to recipients in the network who have included the sender on the whitelist in a predetermined time period divided by a second number of e-mail messages sent by an any sender using the final domain name to users in the network in the predetermined time period;

b) determining a ratio of a first number of recipients in the network who have included the sender on the whitelist divided by a second number of unique recipients in the network who received e-mails from any sender using the final domain name in a predetermined time period;

c) determining a ratio of a first number of times in a predetermined time interval a message from any sender using the final domain name was moved from a whitelist to a blacklist divided by a second number of times a message from any sender using the final domain name was moved from a whitelist to a blacklist;

d) determining a ratio of a first number of times in a predetermined time interval a message from any sender using the final domain name was moved from a blacklist to a whitelist divided by a second number of times a message from any sender using the final domain name was moved from a blacklist to a whitelist;

e) determining a ratio of a first number of unique users within the network who whitelisted any sender using the final domain name within a predetermined time period compared to a second number of unique users within the network who blacklisted any sender using the final domain name within the predetermined time period;

f) determining a ratio reflecting whether any sender using the final domain name sends a majority of messages to recipients who have included the sender on the whitelist;

g) determining a ratio reflecting a first number of wanted messages sent by any sender using the final domain name compared to a second number of unwanted or total messages sent by any sender using the final domain name;

h) determining a difference between a first number of wanted messages sent by any sender using the final domain name and a second number of unexpected messages sent by any sender using the final domain name;

i) determining a difference between a first number of times a user whitelisted a message from any sender using the final domain name and a second number of times a user blacklisted a message from any sender using the final domain name;

j) determining a difference reflecting whether any sender using the final domain name sends a majority of messages to recipients who have included the sender on the whitelist;

k) converting any of the above ratios or differences to a score indicating the likelihood the message is unsolicited e-mail; and

l) applying the score to the appropriate message in the spam folder.

13. The method of claim 1 wherein compiling statistics includes at least one of the following:

a) determining a ratio of a first number e-mail messages sent by any sender using an IP path to recipients in the network who have included the sender on the whitelist in a predetermined time period divided by a second number of e-mail messages sent by an any sender using the IP path to users in the network in the predetermined time period;

b) determining a ratio of a first number of recipients in the network who have included the sender on the whitelist divided by a second number of unique recipients in the network who received e-mails from any sender using the IP path in a predetermined time period;

c) determining a ratio of a first number of times in a predetermined time interval a message from any sender using the IP path was moved from a whitelist to a blacklist divided by a second number of times a message from any sender using the IP path was moved from a whitelist to a blacklist;

d) determining a ratio of a first number of times in a predetermined time interval a message from any sender using the IP path was moved from a blacklist to a whitelist divided by a second number of times a message from any sender using the IP path was moved from a blacklist to a whitelist;

e) determining a ratio of a first number of unique users within the network who whitelisted any sender using the IP path within a predetermined time period compared to a second number of unique users within the network who blacklisted any sender using the IP path within the predetermined time period;

f) determining a ratio reflecting whether any sender using the IP path sends a majority of messages to recipients who have included the sender on the whitelist;

g) determining a ratio reflecting a first number of wanted messages sent by any sender using the IP path compared to a second number of unwanted or total messages sent by any sender using the IP path;

h) determining a difference between a first number of expected messages sent by any sender using the IP path and a second number of unexpected messages sent by any sender using the IP path;

i) determining a difference between a first number of times a user whitelisted a message from any sender using the IP path and a second number of times a user blacklisted a message from any sender using the IP path;

j) determining a difference reflecting whether any sender using the IP path sends a majority of messages to recipients who have included the sender on the whitelist;

k) converting any of the above ratios or differences to a score indicating the likelihood the message is unsolicited e-mail; and

l) applying the score to the appropriate message in the spam folder.

14. The method of claim 1 further comprising revising statistics when a recipient changes a whitelist/blacklist status of one of the following:

a) an actual sender;
b) a final IP address;
c) a final domain name; or
d) an IP path.

15. The method of claim 1 further comprising setting a predetermined threshold for accepting messages based on statistics associated with one of the following:

- a) an actual sender;
- b) a final IP address;
- c) a final domain name; or
- d) an IP path.

16. The method of claim 15 further comprising accepting messages when information about the message exceeds the predetermined threshold.

17. The method of claim 15 further comprising setting a low threshold to differentiate wanted messages from unsolicited messages, wherein the low threshold is either:

a) greater than one percent of a number of messages are accepted, wherein the messages are characterized by one of the following:

- i) an actual sender;
- ii) a final IP address;
- iii) a final domain name; or
- iv) an IP path;

b) greater than one percent of a number of unique users accepting a message characterized by one of the following:

- i) an actual sender;
- ii) a final IP address;
- iii) a final domain name; or
- iv) an IP path.

18. The method of claim 1 further comprising monitoring a recipient's spam folder at predetermined intervals to determine whether messages should be released.

19. The method of claim 18 further comprising automatically releasing the message from the spam folder when the reputation of one of the following:

a) an actual sender;
b) a final IP address;
c) a final domain name; or
d) an IP path;

passes a predetermined threshold.

20. The method of claim 18 further comprising reevaluating the spam folder immediately before it is displayed to the recipient such that information about messages in the spam folder is current when viewed by the recipient.

21. The method of claim 14 wherein manual reversal of the whitelist/blacklist status of one of the following:

a) an actual sender;
b) a final IP address;
c) a final domain name; or
d) an IP path;

is more heavily weighted when revising the statistics.

22. The method of claim 5 wherein information about at least one of the following:

a) the final IP address;
b) the final domain name; and
c) the IP path;

is sent to the recipient when there is insufficient information about the actual sender.

23. The method of claim 1 further comprising using statistics compiled at the at least one database to compute a score indicating a likelihood that the received message is unsolicited e-mail.

24. The method of claim 15 further comprising each user setting a predetermined personalized spam threshold, wherein an incoming message that exceeds the spam threshold is sent to a folder designated to hold spam messages.

25. The method of claim 15 further comprising each user setting a predetermined personalized delete threshold, wherein an incoming message that exceeds the delete threshold is deleted.

26. The method of claim 1 further comprising maintaining at either the central database or the at least two centrally-maintained databases at least four of the following values:

a) a number of messages which were explicitly ranked good;

b) a number of messages which were implicitly ranked good;

c) a number of messages whose ranking is unknown;

d) a number of messages which were explicitly ranked bad; and

e) a number of messages which were implicitly ranked bad;

wherein the values are based on messages having the same information about the sender including one of the following:

i) an actual sender;

ii) a final IP address used by the sender;

iii) a final domain name used by the sender; or

iv) an IP path used by the sender.

27. The method of claim 26 wherein the values represent one of the following:

a) message counts; or

b) ratings of unique users within the network.

28. The method of claim 27 further comprising at least four of the values being returned to the recipient to allow the recipient to apply different weights to a message in order to categorize the message.

29. The method of claim 1 further comprising evaluating an unknown sender based on statistics of one of the following:

a) a known final IP address used by the sender; or

b) a known final domain name used by the sender.

30. The method of claim 1 further comprising evaluating an unknown sender using either a known final IP address or a known final domain name based on statistics about other new senders using either the known final IP address or the known final domain.

31. The method of claim 1 further comprising giving an unknown final IP address or final domain name an initial good rating.

32. The method of claim 1 further comprising giving an unknown final IP address or domain name an initial rating based on the length of time the network has been in operation.

33. The method of claim 4 further comprising older members of the network overwriting a new member's message ratings when the new member's ratings are inconsistent when compared to other member's ratings.

34. The method of claim 23 wherein a final message score is determined by one of the following:

a) an average of two scores for a message; or

b) a product of two scores for the message;

wherein the scores for messages are based on statistics associated with a least two of the following:

i) an actual sender of the message;

ii) a final IP address used by the sender;

iii) a final domain name used by the sender; or

iv) an IP path used by the sender.

35. The method of claim 1 wherein personal statistics are checked at the local database before global statistics at either the central database or the at least two centrally-maintained databases are checked.

36. The method of claim 1 further comprising rating a sender by:

a) releasing small numbers a sender's messages to recipients; and

b) monitoring the recipients' classification of these messages.

37. The method of claim 4 further comprising changing one user's rating when other members outvote the user's rating.

38. The method of claim 5 wherein either the central database or the at least two centrally-maintained databases return more than one value to the recipient.

39. The method of claim 1 further comprising monitoring the inbox at predetermined intervals to determine whether messages should remain in the inbox.

40. The method of claim 23 wherein a first score for an unknown sender using a known final IP address or final domain name may be obtained by multiplying a second score for the final IP address or final domain name by a number less than one.

41. The method of claim 1 further comprising categorizing a received message that cannot be rated locally when user activity is observed.

42. The method of claim 23 further comprising using a second formula to compute the score for the message when the message is reevaluated, wherein the second formula differs from a first formula used to compute the previous message score.

43. The method of claim 1 further comprising sending recipients a notification when any sender's reputation changes.